AMENDMENTS

In the Claims

The following is a marked-up version of the claims with the language that is underlined ("___") being added and the language that contains strikethrough ("—") being deleted:

1. (Currently Amended) A secure printing system comprising:

a printing device configured to print information as hard copy, the ~~printer~~ printing device having located therein a remote print system configured to:

provide a user with an encryption key,

receive information encrypted using the encryption key,

decrypt the information with a corresponding decryption key, and

enable the information, once decrypted, to be printed.

2. (Original) The secure printing system of claim 1, wherein said remote print system generates the encryption key and the corresponding decryption key.

3. (Canceled)

4. (Previously Presented) The secure printing system of claim 1, wherein said printing device includes a display device; and

wherein the encryption key is displayed to the user via the display device.

5. (Previously Presented) The secure printing system of claim 1, wherein the remote print system has an address usable for providing information to the remote print system via a communication network; and

wherein the remote print system is configured to provide the user with the address.

6. (Original) The secure printing system of claim 1, further comprising:

a data retrieval/encryption system arranged at a location remote from the remote print system, the data retrieval/encryption system being configured to communicate with the remote print system via a communication network, the data retrieval/encryption system being further configured to receive the encryption key and information corresponding to information that the user intends to print such that the data retrieval/encryption system locates the information that the user intends to print, encrypts the information that the user intends to print using the encryption key, and communicates the information in an encrypted form to the remote print system.

7. (Original) The secure printing system of claim 6, wherein the data retrieval/encryption system is configured to communicate to the user, via the communication network, that information is available for printing such that, if the user desires the information to be printed, the user can obtain an encryption key from the remote print system and communicate the encryption key to the data retrieval/encryption system for use in encrypting the information to be printed.

8. (Previously Presented) The secure printing system of claim 6, further comprising:

a print request system communicating with the data retrieval/encryption system, the print request system being configured to receive the encryption key and information

corresponding to information that the user intends to print such that the print request system communicates the encryption key and the information corresponding to information that the user intends to print to the data retrieval/encryption system.

9. (Original) The secure printing system of claim 8, wherein the print request system is implemented by a portable computing device.

10. (Original) The secure printing system of claim 9, wherein the portable computing device communicates with the data retrieval/encryption system via wireless communication.

11. (Previously Presented) A secure printing system for printing information, the information being stored in memory at a location remote from a user, the information being accessible to the user via a communication network, said secure printing system comprising:

a printing device operative to print information as hard copy, the printing device having contained therein a remote print system, the remote print system being arranged at a location remote from the information and configured to provide a user with an encryption key,

said remote print system being configured to communicate with the communication network such that said remote print system receives information encrypted using said encryption key,

said remote print system being further configured to decrypt said information with a corresponding decryption key, and enable said information, once decrypted, to be printed;

wherein once said information is decrypted using said decryption key, said printing device is enabled to print said information as hard copy.

12. (Original) The secure printing system of claim 11, further comprising:

means for providing the user with said encryption key.

13. (Original) The secure printing system of claim 12, wherein said means for providing the user with said encryption key is a display device.

14. (Canceled)

15. (Currently Amended) A method for secure printing of information transmitted via a communication network, the information being stored in memory at a first location remote from a user, the information being accessible to the user via the communication network, said method comprising:

providing the user with an encryption key from a printing device, the printing device being operative to print information as hard copy;

receiving, at the printing device located at a second location remote from the first location, information encrypted using the encryption key via the communication network;

decrypting the information with a corresponding decryption key using the printing device; and

enabling the information, once decrypted, to be printed by the printing device.

16. (Previously Presented) The method of claim 15, further comprising:

providing the user with an address usable for providing information to the printing device located at the second location via the communication network.

17. (Original) The method of claim 15, wherein the encryption key is provided to the user visually.

18. (Previously Presented) A method for secure printing of information transmitted via a communication network, the information being stored in memory at a first location remote from a user, the information being accessible to the user via the communication network, said method comprising:

enabling an encryption key to be received from a printing device located at a second location remote from the first location;

enabling information that is to be printed to be identified; and

enabling the encryption key and information corresponding to the information that is to be printed to be transmitted to the first location via the communication network such that the information that is to be printed is encrypted using the encryption key, transmitted to the printing device located at the second location via the communication network, decrypted by the printing device using a corresponding decryption key, and printed by the printing device.

19. (Original) The method of claim 18, wherein enabling the encryption key and information corresponding to the information that is to be printed to be transmitted comprises:

enabling the encryption key and information corresponding to the information that is to be printed to be transmitted via wireless communication.

20. (Canceled)